Digital Marketing

Report generated by Nessus™

Sun, 28 Mar 2021 09:50:10 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

digitalmarketing.contact

0	1	8	2	87
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sun Mar 28 03:24:18 2021
End time:	Sun Mar 28 09:50:09 2021

Host Information

DNS Name:	digitalmarketing.contact
IP:	68.65.122.244

Vulnerabilities

122584 - SQLi scanner

Synopsis

The remote host is vulnerable to SQL injection.

Description

The scanner was able to send specially crafted input to one or more endpoints and parameters on the remote host that resulted in an injection into a SQL query, allowing arbitrary SQL statements to be executed on the remote host.

Solution

In the case of a third party product, the vendor should be notified of this vulnerability. In the case of a custom web application, the application should be updated to use parameterized queries, which prevent an attacker from being able to inject special characters that can be used to break out of the intended context and execute SQL statements.

Risk Factor

High

CVSS v3.0 Base Score

8.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L)

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin Information

Published: 2019/03/04, Modified: 2021/01/15

Plugin Output

tcp/2096/www

```
Injection found on /application/application/application/ in the following parameters :
  login_only

Injection was verified with "SELECT @@version" which yielded :
  Qjz0..
.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2021/01/11

Plugin Output

tcp/2096/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

18391 - SMTP Server Non-standard Port Detection

Synopsis

The remote SMTP service is running on a non-standard port.

Description

This SMTP server is running on a non-standard port. This might be a backdoor set up by attackers to send spam or even control of a targeted machine.

See Also

http://www.icir.org/vern/papers/backdoor/

Solution

Check and clean the configuration.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2005/05/29, Modified: 2017/12/01

Plugin Output

tcp/26/smtp

```
  Banner : 220-premium73.web-hosting.com ESMTP Exim 4.94 #2 Sun, 28 Mar 2021 04:28:33 -0400
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
500 unrecognized command
500 unrecognized command
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/21/ftp

```
The identities known by Nessus are :

  www.digitalmarketing.contact
  digitalmarketing.contact

The Common Name in the certificate is :

  *.web-hosting.com

The Subject Alternate Names in the certificate are :

  *.web-hosting.com
  web-hosting.com
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/993

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/993

```

List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     RC4(128)
 SHA1
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/993

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/2096/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/2096/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - https://digitalmarketing.contact:2096/
  - https://digitalmarketing.contact:2096/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/&timestamp=
  - https://digitalmarketing.contact:2096/.
  - https://digitalmarketing.contact:2096/Content-type
  - https://digitalmarketing.contact:2096/GET
  - https://digitalmarketing.contact:2096/POST
  - https://digitalmarketing.contact:2096/application
  - https://digitalmarketing.contact:2096/application/
  - https://digitalmarketing.contact:2096/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/Content-type
  - https://digitalmarketing.contact:2096/application/GET
  - https://digitalmarketing.contact:2096/application/POST
  - https://digitalmarketing.contact:2096/application/application
  - https://digitalmarketing.contact:2096/application/application/
  - https://digitalmarketing.contact:2096/application/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/POST
  - https://digitalmarketing.contact:2096/application/application/application
  - https://digitalmarketing.contact:2096/application/application/application/
  - https://digitalmarketing.contact:2096/application/application/application/
%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/application/POST
  - https://digitalm [...]
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

Plugin Output

tcp/26/smtp

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 26 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/993

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
 SHA1
    AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2020/06/12

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - www.digitalmarketing.contact
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/21098/ssh

```
Give Nessus credentials to perform local checks.
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF	CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'pass' parameter of the /login/ CGI :

/login/?pass=tkeihn

-------- output --------


<input type="hidden" id="goto_uri" value="/login/?pass=tkeihn" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing  [...]
------------------------

+ The 'user' parameter of the /login/ CGI :

/login/?user=tkeihn
```

```
-------- output --------


<input type="hidden" id="goto_uri" value="/login/?user=tkeihn" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing  [...]
------------------------

+ The 'pass' parameter of the /login/ CGI :

/login/?pass=tkeihn&user=

-------- output --------


<input type="hidden" id="goto_uri" value="/login/?pass=tkeihn&amp;user="
 />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing  [...]
------------------------

+ The 'user' parameter of the /login/ CGI :

/login/?pass=&user=tkeihn

-------- output --------


<input type="hidden" id="goto_uri" value="/login/?pass=&amp;user=tkeihn"
 />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing  [...]
------------------------

+ The 'locale' parameter of the /application/application/application/. CGI :

/application/application/application/.?locale=tkeihn

-------- output --------


<input type="hidden" id="goto_uri" value="/application/application/appli
cation?locale=tkeihn" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing  [...]
------------------------

+ The 'locale' parameter of the /application/application/application/application/. CGI :

/application/application/application/application/.?locale=tkeihn

-------- output --------


<input type="hidden" id="goto_uri" value="/application/application/appli
cation/applicati [...]
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
Nessus encountered :

  - 1 error involving arbitrary command execution (time based) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 1 error involving blind SQL injection checks :
   . connecting to server: errno=1 (operation timed out)
  - 1 error involving blind SQL injection (time based) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 1 error involving directory traversal (write access) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 4 errors involving persistent XSS checks :
  - 3 errors involving XML injection checks :
   . reading the HTTP status line: errno=1 (operation timed out)
   . connecting to server: errno=1 (operation timed out)
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

web code injection                       : S=23         SP=23        AP=29        SC=6         AC=30

SSI injection                            : S=69         SP=69        AP=87        SC=18        AC=90

directory traversal (extended test)      : S=1173       SP=1173      AP=1479      SC=306
 AC=1530
arbitrary command execution              : S=506        SP=506       AP=638       SC=132
 AC=660
XML injection                            : S=23         SP=23        AP=29        SC=6         AC=30

persistent XSS                           : S=92         SP=92        AP=116       SC=24
 AC=120
HTML injection                           : S=55         SP=55        AP=65        SC=45        AC=65

on site request forgery                  : S=11         SP=11        AP=13        SC=9         AC=13

cross-site scripting (comprehensive test): S=391        SP=391       AP=493       SC=102
 AC=510
arbitrary command execution (time based) : S=138        SP=138       AP=174       SC=36
 AC=180
```

```
SQL injection                            : S=644        SP=644       AP=812       SC=168
 AC=840
local file inclusion                     : S=92         SP=92        AP=116       SC=24
 AC=120
script injection                         : S=11         SP=11        AP=13        SC=9         AC=13

injectable parameter                     : S=46         SP=46        AP=58        SC=12        AC=60

unseen parameters                        : S=805        SP=805       AP=1015      SC=210
 AC=1050
cross-site scripting (extended patterns) : S=66         SP=66        AP=78        SC=54        AC=78

blind SQL injection (4 requests)         : S=92         SP=92        AP=116       SC=24
 AC=120
SQL injection (2nd order)              [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
The following tests timed out without finding any flaw :
- SQL injection (on parameters names)
- directory traversal
- SSI injection
- XSS (on parameters names)
- arbitrary command execution
- directory traversal (extended test)
- SQL injection (2nd order)
- local file inclusion
- XSS (on HTTP headers)
- blind SQL injection
- persistent XSS
- uncontrolled redirection
- cross-site scripting (extended patterns)
- HTML injection
- SQL injection
- cross-site scripting (comprehensive test)
- web code injection
```

```
The following tests were interrupted and did not report all possible flaws :
- injectable parameter
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/03/25

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :

  cpe:/a:mantisbt:mantisbt:
  cpe:/a:openbsd:openssh:5.3 -> OpenBSD  OpenSSH 5.3
```

132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```

Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 14772
Timestamp: 2021-03-28 08:28:49
Port: 443

Plugin ID: 42476
Timestamp: 2021-03-28 08:29:03
Port: 21098

Plugin ID: 14772
Timestamp: 2021-03-28 08:28:50
Port: 993
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 45 allowed.
220-Local time is now 04:28. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/15, Modified: 2021/02/24

Plugin Output

tcp/21/ftp

```
The remote FTP service responded to the 'AUTH TLS' command with a
'234' response code, suggesting that it supports that command.  However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2020/11/06

Plugin Output

tcp/2096/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/80/www

```

Based on tests of each method :
  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/2096/www

```

Based on tests of each method :
```

```
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
  BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
  are allowed on :

  /login

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
  BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
  INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
  OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
  RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
  UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

  /
  /application
  /application/application
  /application/application/application
  /application/application/application/application
  /application/application/application/application/application
  /cPanel_magic_revision_1386192030
  /cPanel_magic_revision_1593501200

- Invalid/unknown HTTP methods are allowed on :

  /
  /application
  /application/application
  /application/application/application
  /application/application/application/application
  /application/application/application/application/application
  /cPanel_magic_revision_1386192030
  /cPanel_magic_revision_1593501200
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/2096/www

```
The remote web server type is :

Apache
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
The server supports direct HTTP/2 connections
without encryption.
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
68.65.122.244 resolves as premium73-1.web-hosting.com.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  date: Sun, 28 Mar 2021 09:23:14 GMT
  server: Apache
  location: https://digitalmarketing.contact/
  content-length: 241
  content-type: text/html; charset=iso-8859-1
  connection: close

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://digitalmarketing.contact/">here</a>.</p>
</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2096/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Sun, 28 Mar 2021 09:23:22 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: webmailsession=%3a6iNK9nuPOReED1cp%2c73a8ca7df6f1c2d5788a8dc088ea31b5; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=digitalmarketing.contact; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.digitalmarketing.contact; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.digitalmarketing.contact; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=digitalmarketing.contact; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.digitalmarketing.contact; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2096
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.digitalmarketing.contact; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Mon, 28-Mar-2022 09:23:22 GMT; path=/;
 port=2096; secure
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 39727

Response Body :

 [...]
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
  Request         : http://digitalmarketing.contact/
  HTTP response   : HTTP/1.1 301 Moved Permanently
  Redirect to     : https://digitalmarketing.contact/
  Redirect type   : 30x redirect


Note that Nessus did not receive a 200 OK response from the
last examined redirect.
```

11652 - MantisBT Detection

Synopsis

The remote web server contains a bug tracking application written in PHP.

Description

MantisBT, an open source bug tracking application written in PHP and using a MySQL back-end, was detected on the remote host.

See Also

http://www.mantisbt.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/05/27, Modified: 2020/09/16

Plugin Output

tcp/2096/www

```
Nessus detected 2 installs of MantisBT:

  URL     : https://digitalmarketing.contact:2096/mantis
  Version : unknown

  URL     : https://digitalmarketing.contact:2096/mantisbt
  Version : unknown
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://digitalmarketing.contact:2096/
  - https://digitalmarketing.contact:2096/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/&timestamp=
  - https://digitalmarketing.contact:2096/.
  - https://digitalmarketing.contact:2096/Content-type
  - https://digitalmarketing.contact:2096/GET
  - https://digitalmarketing.contact:2096/POST
  - https://digitalmarketing.contact:2096/application
  - https://digitalmarketing.contact:2096/application/
  - https://digitalmarketing.contact:2096/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/Content-type
  - https://digitalmarketing.contact:2096/application/GET
  - https://digitalmarketing.contact:2096/application/POST
  - https://digitalmarketing.contact:2096/application/application
  - https://digitalmarketing.contact:2096/application/application/
  - https://digitalmarketing.contact:2096/application/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/POST
  - https://digitalmarketing.contact:2096/application/application/application
  - https://digitalmarketing.contact:2096/application/application/application/
  - https://digitalmarketing.contact:2096/application/application/application/
%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/application/POST
  - http [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://digitalmarketing.contact:2096/
  - https://digitalmarketing.contact:2096/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/&timestamp=
  - https://digitalmarketing.contact:2096/.
  - https://digitalmarketing.contact:2096/Content-type
  - https://digitalmarketing.contact:2096/GET
  - https://digitalmarketing.contact:2096/POST
  - https://digitalmarketing.contact:2096/application
  - https://digitalmarketing.contact:2096/application/
  - https://digitalmarketing.contact:2096/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/Content-type
  - https://digitalmarketing.contact:2096/application/GET
  - https://digitalmarketing.contact:2096/application/POST
  - https://digitalmarketing.contact:2096/application/application
  - https://digitalmarketing.contact:2096/application/application/
  - https://digitalmarketing.contact:2096/application/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/POST
  - https://digitalmarketing.contact:2096/application/application/application
  - https://digitalmarketing.contact:2096/application/application/application/
  - https://digitalmarketing.contact:2096/application/application/application/
%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/application/POST
  - https://digitalmarketing.con [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/25

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/26/smtp

```
Port 26/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/53

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/110

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/143

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/993

```
Port 993/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/2096/www

```
Port 2096/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/01/15

Plugin Output

tcp/21098/ssh

```
Port 21098/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/01/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.13.1
Plugin feed version : 202103271111
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
```

```
Ping RTT : 303.096 ms
Thorough tests : yes
Experimental tests : no
Paranoia level : 1
Report verbosity : 2
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2021/3/28 3:24 EDT
Scan duration : 23127 sec
```

50350 - OS Identification Failed

Synopsis

It was not possible to determine the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2020/01/22

Plugin Output

tcp/0

```

If you think these signatures would help us improve OS fingerprinting,
please send them to :

  os-signatures@nessus.org

Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.

HTTP:!:server: Apache

SMTP:!:220-premium73.web-hosting.com ESMTP Exim 4.94 #2 Sun, 28 Mar 2021 04:28:33 -0400
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
500 unrecognized command
500 unrecognized command
SSLcert:!:i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/
CN:digitalmarketing.contact
105180799bdad9e3c31c5886ee7a0c889c8ec7fe
i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:digitalmarketing.contact
105180799bdad9e3c31c5886ee7a0c889c8ec7fe

SinFP:!:
   P1:B11013:F0x12:W65535:O0204ffff:M1460:
   P2:B11013:F0x12:W65535:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181310_7_p=443R
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF	IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2020/09/22

Plugin Output

tcp/0

```
Port 110 was detected as being open initialy but was found unresponsive later.
```

```
 It is now open.
Port 2096 was detected as being open but is now unresponsive
Port 143 was detected as being open initialy but was found unresponsive later.
 It is now open.
Port 21 was detected as being open but is now closed
Port 25 was detected as being open initialy but was found unresponsive later.
 It is now open.
Port 53 was detected as being open initialy but was found unresponsive later.
 It is now open.
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/993

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/2096/www

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2020/06/12

Plugin Output

tcp/0

```
The remote host is up
The remote host replied to an ICMP echo packet
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

tcp/26/smtp

```
The following authentication methods are advertised by the SMTP
server without encryption :
  LOGIN
  PLAIN
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/26/smtp

```
Remote SMTP server banner :

220-premium73.web-hosting.com ESMTP Exim 4.94 #2 Sun, 28 Mar 2021 04:28:33 -0400
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
500 unrecognized command
500 unrecognized command
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/26/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Common Name: digitalmarketing.contact

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 FF EC 0C C3 D5 07 B5 E9 46 0E 90 D9 5E 72 D8 4E

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Feb 15 00:00:00 2021 GMT
Not Valid After: Feb 15 23:59:59 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A9 78 43 02 98 E9 BC 92 59 D0 B7 D5 42 58 D3 FF 22 4A 8E
            ED 38 12 F7 29 99 7C 0D 8B B5 14 6B 06 27 3C 1B 92 EA B2 AC
            19 6A DB B3 47 F3 01 7F 2B 84 96 D2 B4 17 46 E0 11 A4 47 1D
            57 18 1B 01 AE 0F 1A 15 93 63 22 7C 4E B2 29 36 C9 49 D1 8F
            6A 53 CA 41 A8 DA D1 23 B4 25 33 85 31 D9 B7 0A 1B 04 81 F1
            D0 FF 32 35 35 DB C0 99 04 6F 14 C2 7B 80 F5 A9 D7 61 0A 2E
            61 0F 97 10 94 C4 8C C9 A2 E4 29 D4 C7 F7 82 3B 9E B1 CE A0
            3C 42 D8 FB B5 79 64 44 3C 9D A0 B6 E1 C5 91 3B 12 AF 8E 4D
            15 A4 54 35 B6 3D 8A 9C 7C FE 89 FE D8 08 28 54 77 05 8F C0
            0D 0F F0 25 21 2D 57 7D BA F2 59 7D 26 BD E5 47 E4 A5 54 5B
            7F 57 8E 98 F9 4B D5 63 90 9F 79 60 87 ED 97 40 1D 12 EF 1A
            BC 95 1E F3 C3 10 67 C5 85 1E EC BB E8 EE 6F D7 13 DD A6 71
            58 B0 12 A7 F6 0B 9A A0 82 BC 49 31 25 B4 E3 0D 81
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 84 3F 7E EF DF DA 61 15 09 72 0D B6 41 5E 97 7C FA 4D A9
           58 98 78 39 AC 67 D8 9D D9 21 9E B9 32 E3 77 42 AE EC 24 FC
           E9 EB 80 C7 43 38 68 FA 86 D6 BF 18 13 3E E8 13 BA AF C8 FD
           5B F4 C4 04 F1 41 9A 41 80 61 9A 63 79 34 7D B1 67 B8 D6 B9
           30 0B C6 C5 97 01 F5 38 84 28 8C 14 11 94 30 8F 92 17 D7 1E [...]
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/21098/ssh

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes192-ctr
  aes256-ctr

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes192-ctr
  aes256-ctr

The server supports the following options for mac_algorithms_client_to_server :

  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha2-256
  hmac-sha2-512

The server supports the following options for mac_algorithms_server_to_client :

  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha2-256
  hmac-sha2-512

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/21098/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/21098/ssh

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,password
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/21/ftp

```
This port supports TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/993

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/2096/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/21/ftp

```

The host name known by Nessus is :

  digitalmarketing.contact

The Common Name in the certificate is :

  *.web-hosting.com

The Subject Alternate Names in the certificate are :

  *.web-hosting.com
  web-hosting.com
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/21/ftp

```
Subject Name:

Common Name: *.web-hosting.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 D8 9E AF 28 18 4E 98 1A 84 C8 54 B7 82 A2 EC 9E

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 07 00:00:00 2020 GMT
Not Valid After: Apr 05 23:59:59 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 BA 32 8C 41 1A DE FB 13 20 A1 C2 48 18 DF E4 EA D8 F9
            D7 70 18 F0 15 AC 4F 55 1F BD E6 1B EC 4E 9C E3 0C CF E9 75
            0B 10 C9 BB 5A 9B 5C 48 87 5E B7 50 5D C7 0D 7D 48 8B 4B 8F
            3F C7 A7 10 B8 B9 DC 21 BC 31 F9 23 D7 33 B3 69 6F 39 D2 C7
            26 81 C7 66 96 B7 F4 4C 03 6D E4 BE 52 65 6E A3 A7 88 50 05
            83 5B E7 76 11 11 F8 DA EA 0E A8 8C 3A 83 2A B0 A5 16 33 DE
            76 0E F5 97 71 35 74 ED C5 DA 23 DE 9D B1 97 C7 6E C4 3A 3F
            28 65 B8 01 5C DE CE FE 04 63 FB FD F0 FD A3 F2 1C CB A1 0C
            D3 7C 5F C4 BF 9E 48 C6 4C 5D B5 1F A4 D6 33 E4 15 60 58 62
            0D B4 E5 80 59 27 23 CE C3 5C D8 D5 33 F0 61 16 CD 5D 7E ED
            B2 3A BE C9 DC BE 28 FE 82 5C 79 9D E4 E6 D9 CD A1 DE 56 F8
            C7 EB DA 38 B4 8E 3C FD D7 85 01 34 F2 99 A1 B7 A2 E6 B0 E8
            60 AC 21 C9 F3 94 C7 6F F9 C4 84 07 2F B9 82 DF 0B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 1D 48 A4 1F 68 2D 99 E7 EA 72 B7 9D D4 86 C3 45 B3 B5 49
           18 E8 33 C0 81 6D FA 4B E6 47 45 6C D8 68 74 34 61 0A 16 90
           54 67 DC A4 71 5B 39 D5 38 0D AC 6E DB 44 29 4D 90 22 D3 35
           3E 9F BF 03 63 DE 83 51 50 49 89 1B 0E FE D4 E2 31 4D 39 66
           F8 CF 74 0C 7F B2 83 0A F3 AE 26 3B 96 7A 4A F5 57 B8 4C 64
           C6 97 B4 C5 98 15 EB 65 6D 9B CF 09 48 5D E9 2B DB 76 DF 9A
           E2 3C 65 8E F2 47 2E 37 30 D1 4F 68 14 67 6A 0B 49 91 20 A5
           71 3C 99 17 A0 D3 24 90 46 5A 0 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/993

```
Subject Name:

Common Name: digitalmarketing.contact

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 FF EC 0C C3 D5 07 B5 E9 46 0E 90 D9 5E 72 D8 4E

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 15 00:00:00 2021 GMT
Not Valid After: Feb 15 23:59:59 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A9 78 43 02 98 E9 BC 92 59 D0 B7 D5 42 58 D3 FF 22 4A 8E
            ED 38 12 F7 29 99 7C 0D 8B B5 14 6B 06 27 3C 1B 92 EA B2 AC
            19 6A DB B3 47 F3 01 7F 2B 84 96 D2 B4 17 46 E0 11 A4 47 1D
            57 18 1B 01 AE 0F 1A 15 93 63 22 7C 4E B2 29 36 C9 49 D1 8F
            6A 53 CA 41 A8 DA D1 23 B4 25 33 85 31 D9 B7 0A 1B 04 81 F1
            D0 FF 32 35 35 DB C0 99 04 6F 14 C2 7B 80 F5 A9 D7 61 0A 2E
            61 0F 97 10 94 C4 8C C9 A2 E4 29 D4 C7 F7 82 3B 9E B1 CE A0
            3C 42 D8 FB B5 79 64 44 3C 9D A0 B6 E1 C5 91 3B 12 AF 8E 4D
            15 A4 54 35 B6 3D 8A 9C 7C FE 89 FE D8 08 28 54 77 05 8F C0
            0D 0F F0 25 21 2D 57 7D BA F2 59 7D 26 BD E5 47 E4 A5 54 5B
            7F 57 8E 98 F9 4B D5 63 90 9F 79 60 87 ED 97 40 1D 12 EF 1A
            BC 95 1E F3 C3 10 67 C5 85 1E EC BB E8 EE 6F D7 13 DD A6 71
            58 B0 12 A7 F6 0B 9A A0 82 BC 49 31 25 B4 E3 0D 81
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 84 3F 7E EF DF DA 61 15 09 72 0D B6 41 5E 97 7C FA 4D A9
           58 98 78 39 AC 67 D8 9D D9 21 9E B9 32 E3 77 42 AE EC 24 FC
           E9 EB 80 C7 43 38 68 FA 86 D6 BF 18 13 3E E8 13 BA AF C8 FD
           5B F4 C4 04 F1 41 9A 41 80 61 9A 63 79 34 7D B1 67 B8 D6 B9
           30 0B C6 C5 97 01 F5 38 84 28 8C 14 11 94 30 8F 92 17 D7 1E
           32 4D DB 77 16 42 29 53 A2 C0 44 06 EF 7A 06 44 38 41 14 58
           67 F6 8E BF CF 20 A6 36 5F 44 D6 5E 8D 72 08 F0 53 69 9B 0A
           D8 7C 0D 2C 75 7E 91 0C  [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2096/www

```
Subject Name:

Common Name: digitalmarketing.contact

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 FF EC 0C C3 D5 07 B5 E9 46 0E 90 D9 5E 72 D8 4E

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 15 00:00:00 2021 GMT
Not Valid After: Feb 15 23:59:59 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A9 78 43 02 98 E9 BC 92 59 D0 B7 D5 42 58 D3 FF 22 4A 8E
            ED 38 12 F7 29 99 7C 0D 8B B5 14 6B 06 27 3C 1B 92 EA B2 AC
            19 6A DB B3 47 F3 01 7F 2B 84 96 D2 B4 17 46 E0 11 A4 47 1D
            57 18 1B 01 AE 0F 1A 15 93 63 22 7C 4E B2 29 36 C9 49 D1 8F
            6A 53 CA 41 A8 DA D1 23 B4 25 33 85 31 D9 B7 0A 1B 04 81 F1
            D0 FF 32 35 35 DB C0 99 04 6F 14 C2 7B 80 F5 A9 D7 61 0A 2E
            61 0F 97 10 94 C4 8C C9 A2 E4 29 D4 C7 F7 82 3B 9E B1 CE A0
            3C 42 D8 FB B5 79 64 44 3C 9D A0 B6 E1 C5 91 3B 12 AF 8E 4D
            15 A4 54 35 B6 3D 8A 9C 7C FE 89 FE D8 08 28 54 77 05 8F C0
            0D 0F F0 25 21 2D 57 7D BA F2 59 7D 26 BD E5 47 E4 A5 54 5B
            7F 57 8E 98 F9 4B D5 63 90 9F 79 60 87 ED 97 40 1D 12 EF 1A
            BC 95 1E F3 C3 10 67 C5 85 1E EC BB E8 EE 6F D7 13 DD A6 71
            58 B0 12 A7 F6 0B 9A A0 82 BC 49 31 25 B4 E3 0D 81
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 84 3F 7E EF DF DA 61 15 09 72 0D B6 41 5E 97 7C FA 4D A9
           58 98 78 39 AC 67 D8 9D D9 21 9E B9 32 E3 77 42 AE EC 24 FC
           E9 EB 80 C7 43 38 68 FA 86 D6 BF 18 13 3E E8 13 BA AF C8 FD
           5B F4 C4 04 F1 41 9A 41 80 61 9A 63 79 34 7D B1 67 B8 D6 B9
           30 0B C6 C5 97 01 F5 38 84 28 8C 14 11 94 30 8F 92 17 D7 1E
           32 4D DB 77 16 42 29 53 A2 C0 44 06 EF 7A 06 44 38 41 14 58
           67 F6 8E BF CF 20 A6 36 5F 44 D6 5E 8D 72 08 F0 53 69 9B 0A
           D8 7C 0D 2C 75 7E 91 0C  [...]
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

See Also

https://tools.ietf.org/html/rfc3279

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

Plugin Output

tcp/21/ftp

```

The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.
```

```
|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

See Also

https://tools.ietf.org/html/rfc3279

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

Plugin Output

tcp/993

```

The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.
```

```
|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

See Also

https://tools.ietf.org/html/rfc3279

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

Plugin Output

tcp/2096/www

```

The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.
```

```
|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/993

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)
```

```
   Name                          Code             KEX           Auth     Encryption             MAC
   ----------------------        ----------       ---           ----     ---------------------  ---
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
SHA1
   AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00 [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2096/www

```

Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/993

```

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA    [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/2096/www

```

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256     [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/993

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
SHA1
   DHE-RSA-AES128-SHA256      [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2096/www

```

Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/21/ftp

```

The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/993

```

The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/2096/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/03/22

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/03/22

Plugin Output

tcp/26/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/03/22

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/03/22

Plugin Output

tcp/2096/www

```
A TLSv1 server answered on this port.
```

tcp/2096/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/03/22

Plugin Output

tcp/21098/ssh

```
An SSH server is running on this port.
```

14772 - Service Detection (2nd Pass)

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem.

Solution

See below

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2011/04/01

Plugin Output

tcp/0

```
doublecheck_std_services identified 1 servicerunning
on top of SSL/TLS.
The transport layer should have been found by find_service.
You should set the "Test SSL based services" option to
"All" or "Known SSL ports".
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/993

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/2096/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2096/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 68.65.122.244 :
10.0.2.15
10.0.2.2
?

Hop Count: 2
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/80/www

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
```

```
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2096/www

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
```

```
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Mon, 28-Mar-2022 08:51:18 GMT
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailsession
Path : /
Value : %3a3UnD7GSkUM5tX9PS%2c0e90cdadcbba070dda89829c16f766ac
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/2096/www

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .digitalmarketing.contact
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Mon, 28-Mar-2022 08:51:18 GMT
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailsession
Path : /
Value : %3a3UnD7GSkUM5tX9PS%2c0e90cdadcbba070dda89829c16f766ac
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/2096/www

```
Potentially sensitive parameters for CGI /resetpass :

user : Potential horizontal privilege escalation - try another user ID

Potentially sensitive parameters for CGI /login/ :

pass : Possibly a clear or hashed password, vulnerable to dictionary attack
user : Potential horizontal privilege escalation - try another user ID
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/2096/www

```
The following sitemap was created from crawling linkable content on the target host :

  - https://digitalmarketing.contact:2096/
  - https://digitalmarketing.contact:2096/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/&timestamp=
  - https://digitalmarketing.contact:2096/.
  - https://digitalmarketing.contact:2096/Content-type
  - https://digitalmarketing.contact:2096/GET
  - https://digitalmarketing.contact:2096/POST
  - https://digitalmarketing.contact:2096/application
  - https://digitalmarketing.contact:2096/application/
  - https://digitalmarketing.contact:2096/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/Content-type
  - https://digitalmarketing.contact:2096/application/GET
  - https://digitalmarketing.contact:2096/application/POST
  - https://digitalmarketing.contact:2096/application/application
  - https://digitalmarketing.contact:2096/application/application/
  - https://digitalmarketing.contact:2096/application/application/%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/POST
  - https://digitalmarketing.contact:2096/application/application/application
  - https://digitalmarketing.contact:2096/application/application/application/
  - https://digitalmarketing.contact:2096/application/application/application/
%2B_detect_timezone()%2B
  - https://digitalmarketing.contact:2096/application/application/application/&timestamp=
  - https://digitalmarketing.contact:2096/application/application/application/Content-type
  - https://digitalmarketing.contact:2096/application/application/application/GET
  - https://digitalmarketing.contact:2096/application/application/application/POST
  - https://digitalmarketing.contact:20 [...]
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/80/www

```

CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://digitalmarketing.contact/asj1c2FmXdi9.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/2096/www

```
The following string will be used :
TYPE="password"
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2096/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2021/01/15

Plugin Output

tcp/2096/www

```

Webmirror performed 81 queries in 548s (0.0147 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : GET
  Argument : locale
   Value: zh_tw
  Argument : login_only
   Value: 1


+ CGI : /resetpass
  Methods : GET,POST
  Argument : debug
  Argument : start
   Value: 1
  Argument : user


+ CGI : /login/
  Methods : POST
  Argument : pass
  Argument : user
```

```
+ CGI : /.
  Methods : GET
  Argument : locale


+ CGI : /application/
  Methods : GET
  Argument : locale
  Argument : login_only
   Value: 1


+ CGI : /application/.
  Methods :
  Argument : locale


+ CGI : /application/application/
  Methods : GET
  Argument : locale
  Argument : login_only
   Value: 1


+ CGI : /application/application/.
  Methods :
  Argument : locale


+ CGI : /application/application/application/
  Methods : GET
  Argument : locale
  Argument : login_only
   Value: 1


+ CGI : /application/application/application/.
  Methods :
  Argument : locale


+ CGI : /application/application/application/application/
  Methods : GET
  Argument : locale
  Argument : login_only
   Value: 1


+ CGI : /application/application/application/application/.
  Methods :
  Argument : locale


+ CGI : /application/application/application/application/application/
  Methods : GET
  Argument : locale
  Argument : login_only
   Value: 1


+ CGI : /application/application/application/application/application/.
  Methods :
  Argument : locale
```

11421 - smtpscan SMTP Fingerprinting

Synopsis

It is possible to fingerprint the remote mail server.

Description

smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2019/11/22

Plugin Output

tcp/26/smtp

```

smtpscan was not able to reliably identify this server. It might be:
Exim 3.35
Exim 4.82
Exim 4.72
Exim 4.10
The fingerprint differs from these known signatures on 2 point(s)

If you know precisely what it is, please send this fingerprint
to smtp-signatures@nessus.org :
:550:250:500:250:501:250:501:214:501:550:500:500:500:250:250
220-premium73.web-hosting.com ESMTP Exim 4.94 #2 Sun, 28 Mar 2021 04:29:08 -0400
```